# Implementation Issues for Electronic Commerce:

What Every Developer Should Know

Aviel D. Rubin
AT&T Labs – Research
180 Park Ave.
Florham Park, NJ 07932
rubin@research.att.com

In the past two years, we have witnessed a proliferation of electronic commerce protocols. Whether we like it or not, these protocols are being implemented all over the place. SET [2] has emerged as the Internet standard for credit card transactions, and has been endorsed by such companies as VISA, Mastercard, IBM, HP, and many more. SSL [3] servers are ubiquitous as the web's answer to secure communication.

Recently, there has been a revival of research into analysis of cryptographic protocols. Significant progress has been made. Model checking techniques and theorem provers are being utilized to run through specifications and find design flaws. The Common Authentication Protocol Specification Language (CAPSL) [1] is emerging as a standard for expressing authentication and key-exchange protocols. The trend is encouraging.

A protocol is usually considered secure after the specification has been thoroughly analyzed. Often, little or no attention is paid to the analysis and correctness of implementations. However, implementation bugs can lead to at least as many security problems as flaws in a design. These are the hardest to prevent or detect.

Implementations of security protocols require experience, care, methodology, and code-review, to mention a few. The implementor must be familiar with the parameters of the cryptography used as well as the system-level issues that could lead to breaches. For example, failure to implement El-Gammal in a large enough group, or poor choice of primes for RSA can result in a totally insecure system. Similarly, failure to clear out temporary buffers where cryptographic operations take place is fatal from the point of view of security. Developers must possess expertise in both cryptography and systems to securely implement protocols, or the security of the specification is irrelevant.

This panel brings together some of the pioneers in the development and deployment of the most popular e-commerce protocols. They will discuss their methodologies and what they think are the most important aspects of developing software that implements these standards. The panel will discuss the pitfalls in the implementation phase, once a secure protocol has been designed and specified. The discussion will focus on assurance of security properties. In particular, the panelists will discuss how to answer the following types of questions:

- How do we know that the secret key is not leaking?
- How do we know that the credit card will only be used for requested purchases?
- How do we evaluate implementations?

There will be short presentations by the panelists followed by questions from the audience.

## References

[1] http://www.jcompsec.mews.org/capsl/

[2] Visa and MasterCard. *Secure Electronic Transactions (SET) Specification*, Book 2: Technical Specifications: http://www.visa.com/set/, February, 1996.

[3] A Freier, P. Karlton, and P. Kocher, *The SSL Protocol Version 3.0*, ftp.netscape.com/pub/review/ssl-spec.tar.Z, March 4, 1996.